Приложение №8
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
обеспечения целостности

1 Общие положения

1.1 Настоящая Политика определяет требования к обеспечению целостности информационной инфраструктуры и информации УФИЦ РАН

2 Контроль целостности программного обеспечения

2.1 В информационной инфраструктуре осуществляется контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

2.2 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, предусматривает:

2.2.1 контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной инфраструктуры;

2.2.2 контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной инфраструктуры;

2.2.3 контроль применения средств разработки и отладки программ в составе программного обеспечения информационной инфраструктуры;

2.2.4 тестирование с периодичностью, установленной оператором функций безопасности средств защиты информации, в том числе с помощью тестпрограмм, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;

2.2.5 обеспечение физической защиты технических средств информационной системы.

2.3 В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

3 Контроль целостности информации, содержащейся в базах данных информационной системы

3.1 В информационной инфраструктуре осуществляется контроль целостности информации, содержащейся в базах данных информационной инфраструктуры, с помощью средства Zabbix.

3.2 Контроль целостности информации, содержащейся в базах данных информационной инфраструктуры, предусматривает:

3.2.1 контроль целостности с постоянной периодичностью структуры базы данных по наличию имен (идентификаторов) и (или) по контрольным суммам программных компонент базы данных в процессе загрузки и (или) динамически в процессе работы информационной инфраструктуры;

3.2.2 контроль целостности с постоянной периодичностью объектов баз данных, определяемых оператором, по контрольным суммам и (или) с использованием криптографических методов в процессе загрузки и (или) динамически в процессе работы информационной инфраструктуры;

3.2.3 обеспечение физической защиты технических средств информационной инфраструктуры, на которых установлена база данных.

3.2.4 обеспечение целостности и сохранности информации, относящейся к деятельности УФИЦ РАН, при увольнении сотрудника контролируется отделом кадров УФИЦ РАН по согласованию с отделом информационных технологий УФИЦ РАН.

4 Обеспечение возможности восстановления программного обеспечения при возникновении нештатных ситуаций

4.1 В УФИЦ РАН предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций, с помощью автоматического резервного копирования данных на сетевые хранилища, защищенные избыточным массивом жестких дисков RAID с оповещением по почте.

4.2 Для обеспечения возможности восстановления программного обеспечения в информационной инфраструктуре приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.

4.3 Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

4.3.1 восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

4.3.2 восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

4.3.3 возврат информационной инфраструктуры в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной инфраструктуры, позволяющих решать задачи по обработке информации.

4.4 В УФИЦ РАН применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.